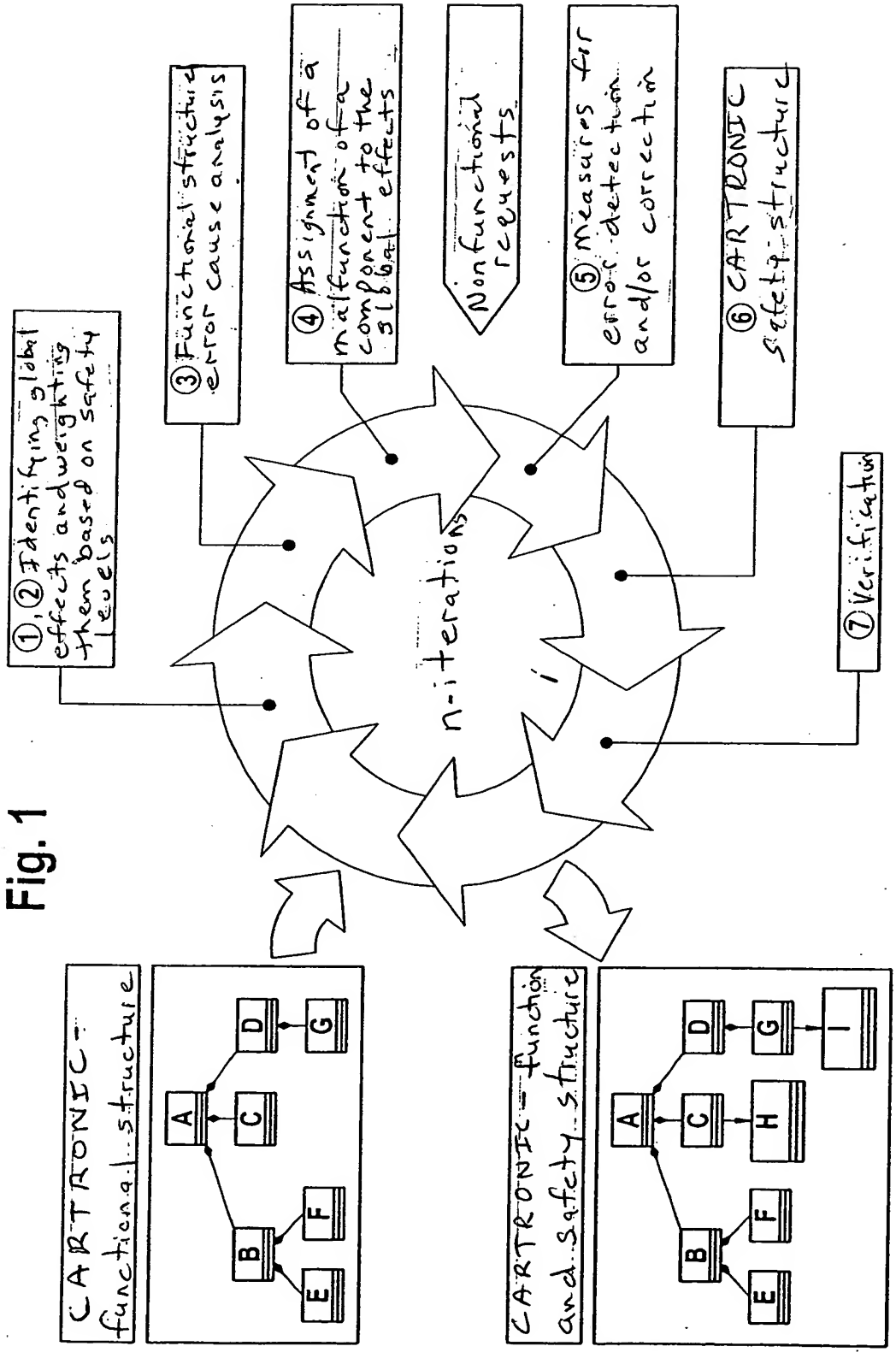
Fig. 1


①,② Identifying global effects and weighting them based on safety levels
③ Functional structure error cause analysis
④ Assignment of a malfunction of a component to the global effects
Nonfunctional requests
⑤ Measures for error detection and/or correction
⑥ CARTRONIC safety structure
⑦ Verification
n-iterations
i
CARTRONIC - functional structure
A
B
C
D
E
F
G
CARTRONIC - function and safety structure
A
B
C
D
E
F
G
H
I

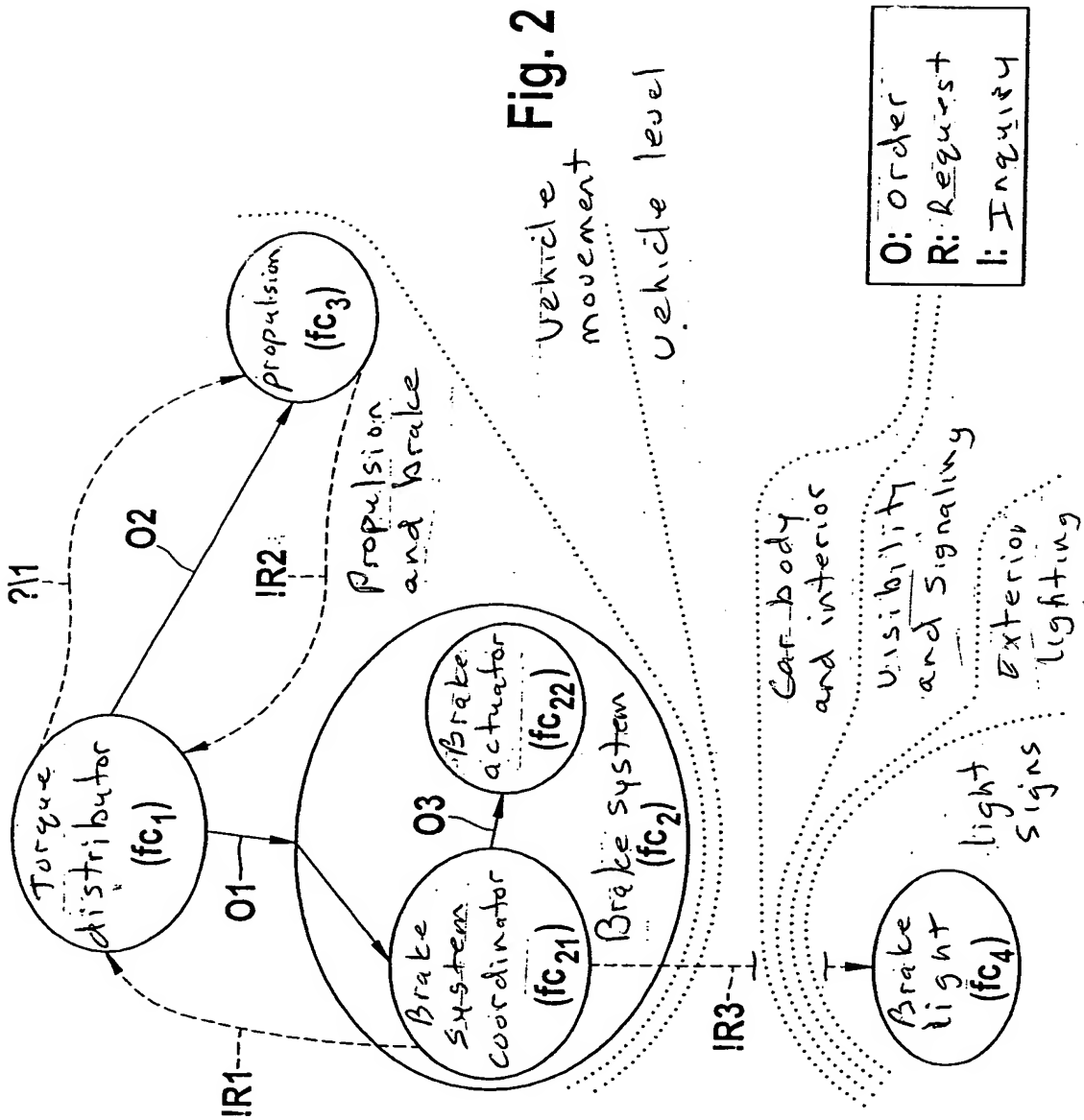

Torque distributor (fc1)
propulsion (fc3)
Brake system coordinator (fc21)
Brake actuator (fc22)
Brake system (fc2)
Brake light (fc4)
?I1
O2
!R2
Propulsion and brake
O1
O3
!R1
!R3
Vehicle movement
vehicle level
Car body and interior
visibility and signaling
light signs
Exterior lighting
O: Order
R: Request
I: Inquiry

Fig. 2

Fig. 3

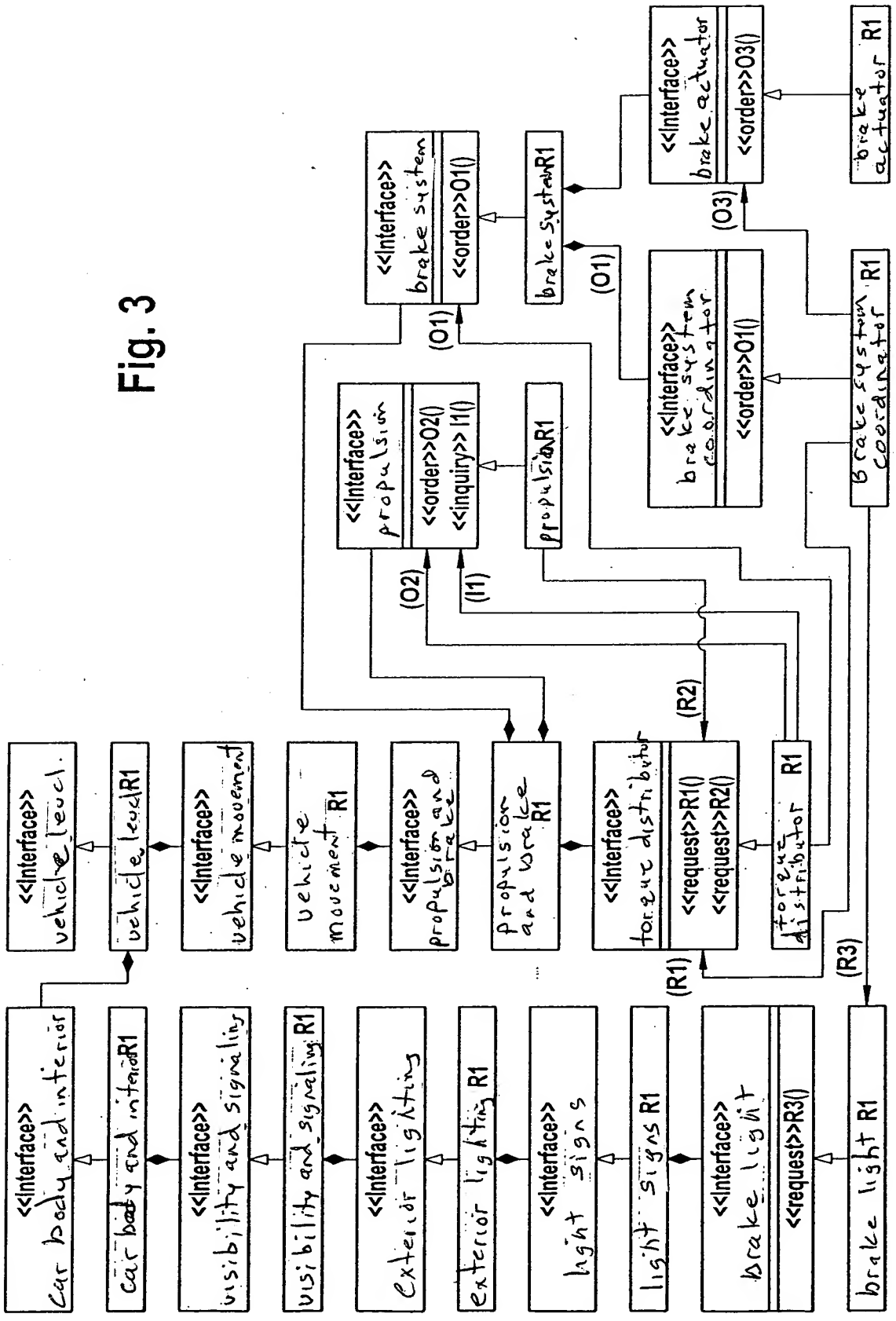

<<Interface>>
car body and interior
car body and interior R1
<<Interface>>
visibility and signaling
visibility and signaling R1
<<Interface>>
exterior lighting
exterior lighting R1
<<Interface>>
light signs
light signs R1
<<Interface>>
brake light
<<request>>R3()
brake light R1
<<Interface>>
vehicle level
vehicle level R1
<<Interface>>
vehicle movement
vehicle movement R1
<<Interface>>
propulsion brake
<<Interface>>
propulsion and brake
propulsion and brake R1
<<Interface>>
torque distributor
<<request>>R1()
<<request>>R2()
torque distributor R1
(R1)
(R2)
(R3)
<<Interface>>
propulsion
<<order>>O2()
<<inquiry>>I1()
propulsion R1
(O2)
(I1)
<<Interface>>
brake system
<<order>>O1()
brake system R1
(O1)
<<Interface>>
brake system coordinator
<<order>>O1()
brake system coordinator R1
(O1)
<<Interface>>
brake actuator
<<order>>O3()
brake actuator R1
(O3)

Fig. 4

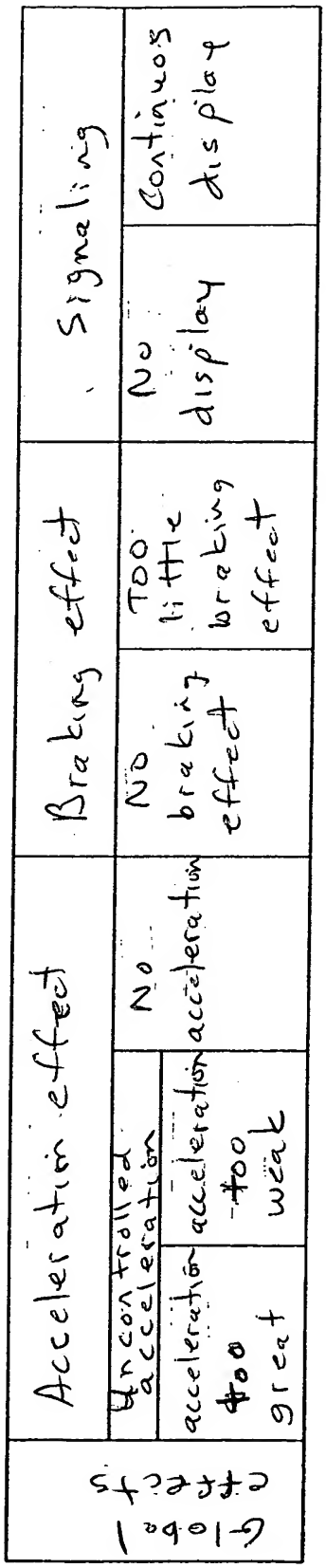

Global effects
Acceleration effect
Uncontrolled acceleration
acceleration too great
acceleration too weak
No acceleration
Braking effect
No braking effect
Too little braking effect
Signaling
No display
Continuous display
Global effects

Fig. 5

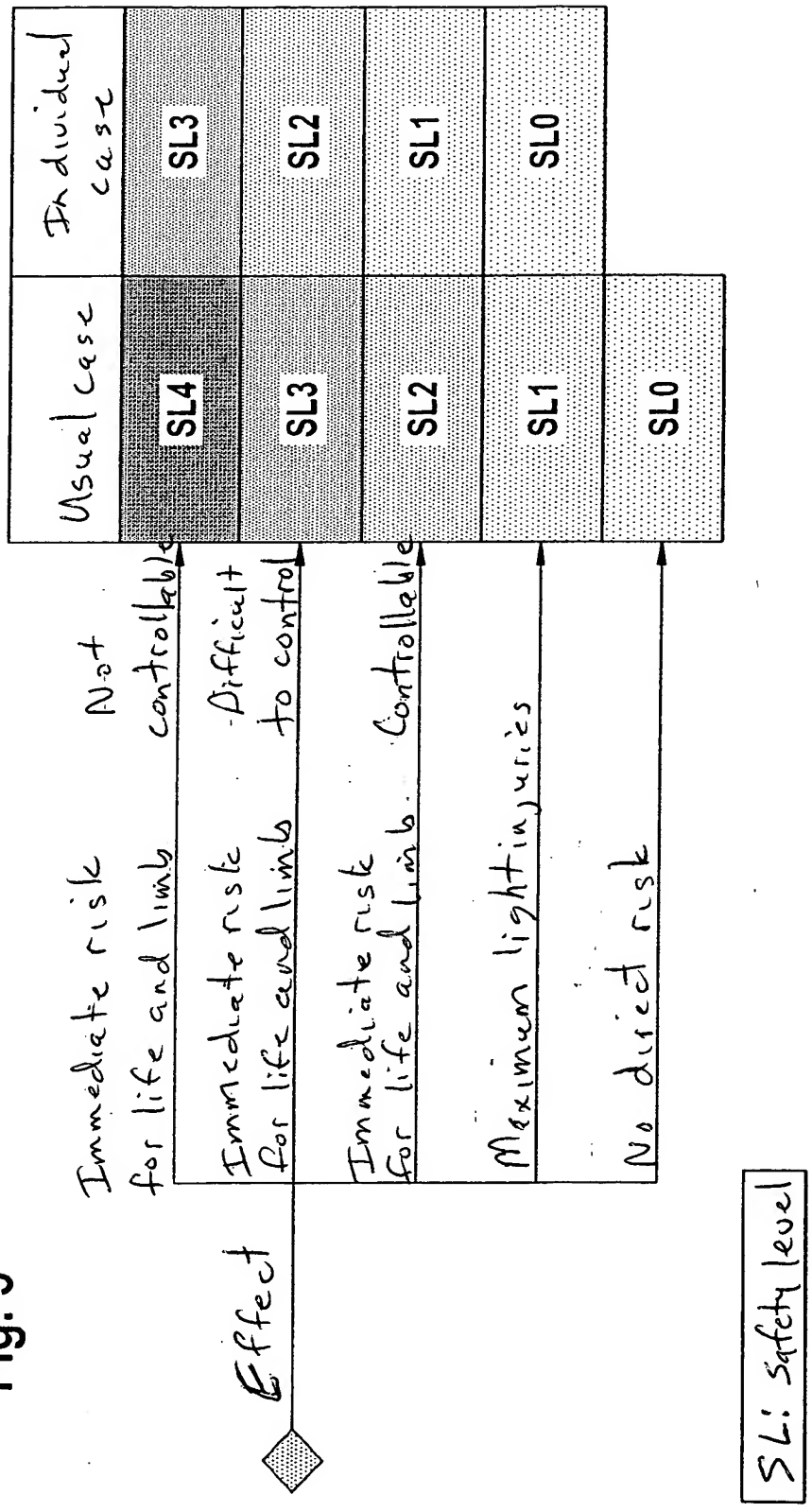
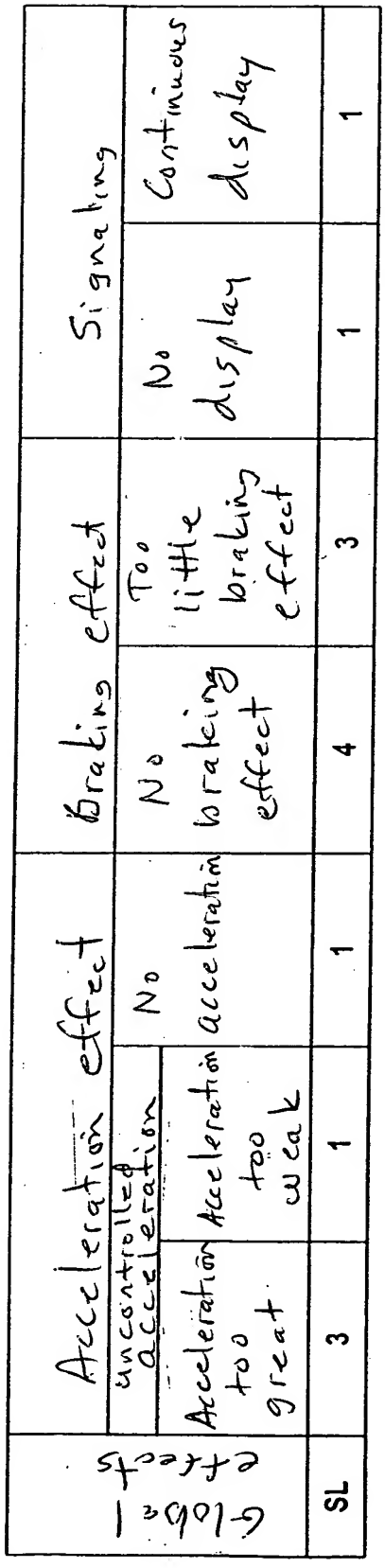

Effect
Immediate risk for life and limb
Not controllable
Immediate risk for life and limb
Difficult to control
Immediate risk for life and limb
Controllable
Maximum lightinjuries
No direct risk
Usual case
Individual case
SL4
SL3
SL3
SL2
SL2
SL1
SL1
SL0
SL0
SL: safety level

Fig. 6


Globe effects
Acceleration effect
Uncontrolled acceleration
Acceleration too great
Acceleration too weak
No acceleration
Braking effect
No braking effect
Too little braking effect
Signaling
No display
Continuous display
SL
3
1
1
4
3
1
1

Global effects	Acceleration effect		Braking effect		Signaling		Malfunction / Functional structure		fc1		fc2		fc21		fc22		fc3		fc4	
	uncontrolled acceleration	No acceleration	No braking effect	Too little braking effect	No display	continuous display			C	M	C	M	C	M	C	M	C	M	C	M
SL	2	1	4	3	1	1														
							fc1		x	R_R1 R_R2 I_I1										
							fc2				x	O_01								
								fc21					x	O_01						
								fc22							x	O_03				
							fc3										x	O_02		
							fc4												x	R_R3

Fig. 7

The following abbreviations are used for the components:

- fc_1 → torque distributor
- fc_2 → brake system
- fc_{21} → brake system coordinator
- fc_{22} → brake actuator
- fc_3 → propulsion
- fc_4 → brake light

Columns C and M in the functional structure stand for:

C: Component
M: Message

10/506372

Global effects	Acceleration effect		Braking effect		Signaling		Malfunction / Functional structure	fc_1		fc_2						fc_3		fc_4	
												fc_{21}		fc_{22}					
	uncontrolled acceleration	NO acceleration	NO braking effect	Too little braking effect	NO display	Continuous display		C	M	C	M	C	M	C	M	C	M	C	M
SL	2	1	4	3	1	1													
							fc_1	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
							fc_2	x	R_R1 R_R2 I_I1	x	O_01					x	O_02		
							fc_{21}	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
							fc_{22}	x	R_R1 R_R2 I_I1			x	O_01	x	O_03 R_R1	x	O_02		
							fc_3	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
							fc_4	x	R_R1 R_R2 I_I1			x	O_01			x	O_02	x	R_R3

The following abbreviations are used for the components:

fc_1 → torque distributor
fc_2 → brake system
fc_{21} → brake system coordinator
fc_{22} → brake actuator
fc_3 → propulsion
fc_4 → brake light

Columns C and M in the functional structure stand for:

C: component
M: message

Fig. 8a

10/506372

Global effects	Acceleration effect		Braking effect		Signaling	
	uncontrolled acceleration	No acceleration	No braking effect	Too little braking effect	No display	continuous display
SL	2	1	4	3	1	1
			X	X		
	X	X				
					X	X

Malfunction / Functional structure	fc_1		fc_2		fc_{21}		fc_{22}		fc_3		fc_4	
	C	M	C	M	C	M	C	M	C	M	C	M
fc_1	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
fc_2	x	R_R1 R_R2 I_I1	x	O_O1					x	O_O2		
fc_{21}	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
fc_{22}	x	R_R1 R_R2 I_I1			x	O_O1	x	O_O3 R_R1	x	O_O2		
fc_3	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
fc_4	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2	x	R_R3

The following abbreviations are used for the components:

fc_1 → torque distributor
fc_2 → brake system
fc_{21} → brake system coordinator
fc_{22} → brake actuator
fc_3 → propulsion
fc_4 → brake light

Columns C and M in the functional structure stand for:
C: component
M: message

Fig. 8b

10/506372

Global effects	Acceleration effect		Braking effect		Signaling		Malfunction / Functional structure		fc_1		fc_2						fc_3		fc_4	
													fc_{21}		fc_{22}					
	uncontrolled acceleration	No acceleration	No braking effect	Too little braking effect	No display	continuous display			C	M	C	M	C	M	C	M	C	M	C	M
SL	2	1	4	3	1	1														
	x	x	x	x	x	x	fc_1		x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
	x	x	x	x	x	x	fc_2		x	R_R1 R_R2 I_I1	x	O_01					x	O_02		
	x	x	x	x	x	x		fc_{21}	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
			x	x				fc_{22}	x	R_R1 R_R2 I_I1			x	O_01	x	O_03 R_R1	x	O_02		
	x	x	x	x	x	x	fc_3		x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
					x	x	fc_4		x	R_R1 R_R2 I_I1			x	O_01			x	O_02	x	R_R3

The following abbreviations are used for the components:

fc_1 → torque distributor
fc_2 → brake system
fc_{21} → brake system coordinator
fc_{22} → brake actuator
fc_3 → propulsion
fc_4 → brake light

Columns C and M in the functional structure stand for:

C: component
M: message

Fig. 8c

10/12

10/506372

Global effects	Acceleration effect		Braking effect		Signaling		SL	Malfunction / Functional structure	fc_1		fc_2						fc_3		fc_4	
													fc_{21}		fc_{22}					
	uncontrolled acceleration	NO acceleration	NO braking effect	TOO LITTLE braking effect	NO display	continuous display			C	M	C	M		M		M		M	C	M
SL	2	1	4	3	1	1														
	x	x	x	x	x	x	4	fc_1	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
	x	x	x	x	x	x	4	fc_2	x	R_R1 R_R2 I_I1	x	O_01					x	O_02		
	x	x	x	x	x	x	4	fc_{21}	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
			x	x			4	fc_{22}	x	I R_R1 R_R2 I_I1			x	O_01	x	O_03	x	O_02		
	x	x	x	x	x	x	4	fc_3	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
					x	x	1	fc_4	x	R_R1 R_R2 I_I1			x	O_01			x	O_02	x	R_R3

Fig. 8d

the following abbreviations are used for the companies

fc_1 → torque distributor
fc_2 → brake system
fc_{21} → brake system coordinator
fc_{22} → brake actuator
fc_3 → propulsion
fc_4 → brake light

Columns C and M in the functional structure stand for:
C: component
M: message

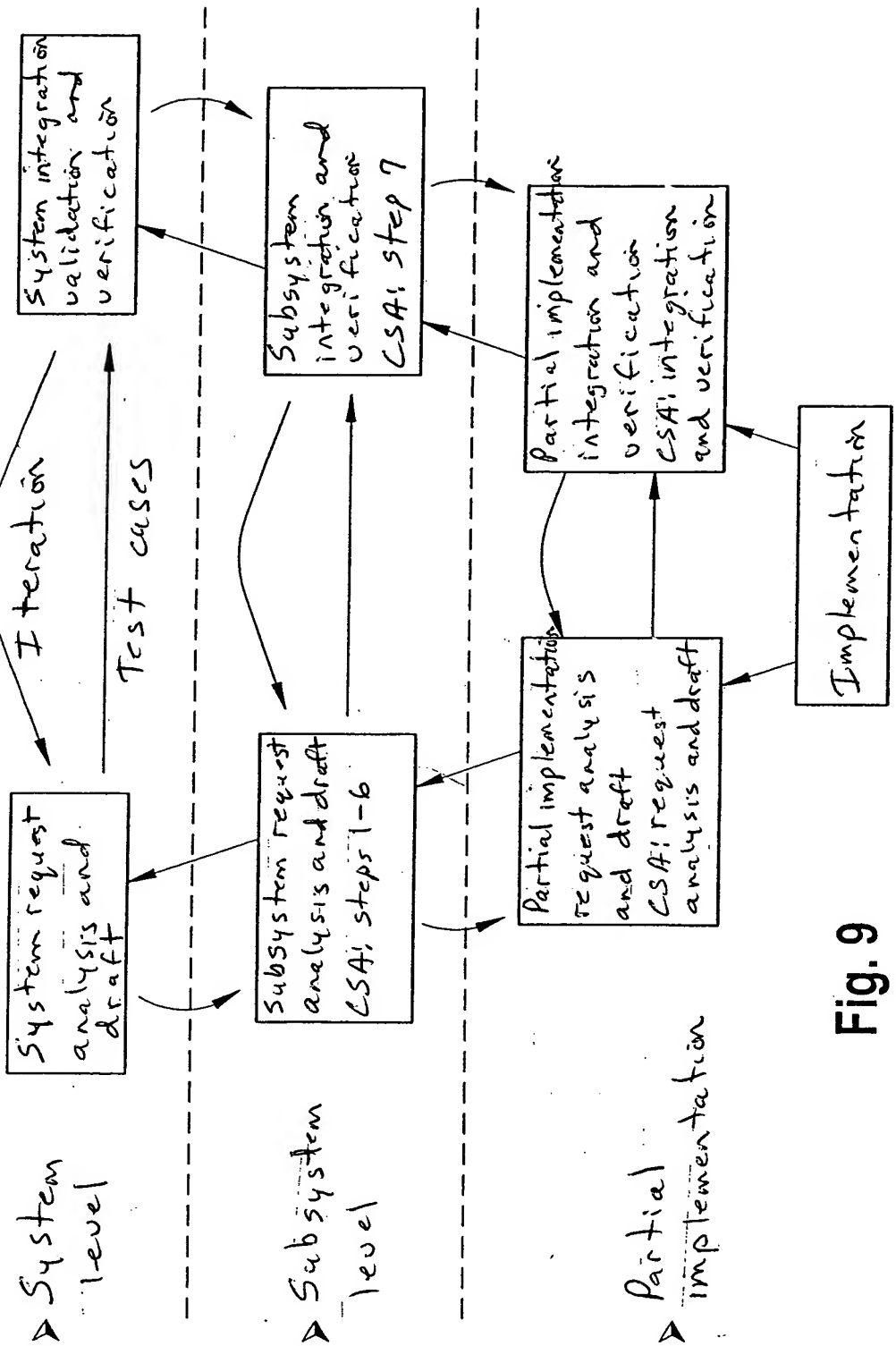

System integration validation and verification
Subsystem integration and verification CSA; step 7
Partial implementation integration and verification CSA; integration and verification
Implementation
Iteration
Test cases
System request analysis and draft
Subsystem request analysis and draft CSA; steps 1-6
Partial implementation request analysis and draft CSA; request analysis and draft
System level
Subsystem level
Partial implementation

Fig. 9